CLAIMS

We claim:

1.   A method of using a .ZIP file as a flexible secure data container, the method comprising the steps of:

5   modifying the standard .ZIP file format to allow for flexible security of the data contained in the file; and

selecting and applying strong encryption algorithms to the data in the file.

2.   The method of claim 1, wherein the strong encryption algorithms include symmetric, asymmetric, or a mixture of symmetric and asymmetric encryption methods.

10   3.   A method of using a standard .ZIP file format as a flexible secure data container through the integration of a plurality of strong encryption methods, the method comprising the steps of:

modifying the standard .ZIP file format to allow for flexible security of the data contained in the file;

15   providing the use of strong encryption algorithms to the data in the files; and

wherein the strong encryption algorithms may include either symmetric or asymmetric encryption methods.

4.   The method of claim 3, wherein the strong encryption algorithms may also include a mixture of symmetric and asymmetric encryption methods.

20   5.   A method of using a standard .ZIP file format and strong encryption methods to flexibly and securely store files, the method comprising the steps of: modifying the standard .ZIP

file format to support strong encryption and a plurality of data encryption algorithms and associated key management processes to produce a highly secure and flexible digital container for storing and transferring confidential electronic data.

6.   The method of claim 5, further comprising the step of supporting the encryption

5   of file characteristics for each file inside a .ZIP file, thereby increasing the level of security available to .ZIP file users.

7.   The method of claim 6, wherein the file characteristics may include the file's name, size, etc.

8.   The method of claim 5, further comprising the step of providing a plurality of

10   methods for validating a digital certificate associated with an encrypted .ZIP file.

9.   A method of strongly encrypting .ZIP files, the method comprising the steps of:

modifying the standard .ZIP file format to allow for flexible security of the data contained in the file;

selecting and applying a strong encryption algorithm to the data in the file; and

15   wherein the process of encrypting the files may include the use of at least one application each of symmetric and asymmetric encryption.

10.   The method of claim 9, wherein the encryption process may also include a mixture of symmetric and asymmetric encryption methods.

11.   The method of claim 9, wherein the encryption process includes the use of at least

20   one password and at least one public/private key.

12.   The method of claim 11 wherein the public/private key encryption utilizes the

X.509 digital certificate standard.

13.   A method of using a .ZIP file as a flexible secure data container, the method

comprising the steps of:

5   creating a data file in a .ZIP file format to allow for flexible security of the data contained

in the file; and

wherein the .ZIP file format supports the selection and implementation of the basic

security functions to be associated with encrypted files.

14.   The method of claim 13, wherein the security functions include message

10   authentication.

15.   The method of claim 13, wherein the security functions include creator

authentication. ,

16.   The method of claim 13, wherein the security functions include non-repudiation.

17.   The method of claim 16, wherein the encryption function further includes time-

15   stamping.

18.   A method of using a .ZIP file as a flexible secure data container, the method

comprising the steps of:

creating a file structure that allows for flexible security of the data contained in the file;

and

20   selecting and applying strong encryption algorithms to the data in the file.

19.   The method of claim 18, wherein the strong encryption algorithms include symmetric, asymmetric, or a mixture of symmetric and asymmetric encryption methods.

20.   A method of using a standard .ZIP file format as a flexible secure data container through the integration of a plurality of strong encryption methods, the method comprising the

5   steps of:

creating a data file structure to allow for flexible security of the data contained in the file;

providing the use of strong encryption algorithms to the data in the files; and

wherein the strong encryption algorithms may include either symmetric or asymmetric

encryption methods.

10   21.   The method of claim 20, wherein the strong encryption algorithms may also

include a mixture of symmetric and asymmetric encryption methods.

22.   A file created in a .ZIP file format comprising:

compressed data;

wherein the data is encrypted using strong encryption algorithms; and

15   wherein the strong encryption algorithms include symmetric, asymmetric, or a mixture of

symmetric and asymmetric encryption methods.

23.   A file created in a .ZIP file format comprising:

archived data;

wherein the data is encrypted using strong encryption algorithms; and

20   wherein the strong encryption algorithms include symmetric, asymmetric, or a mixture of

symmetric and asymmetric encryption methods.

24.   The file of claim 23 wherein the archived data includes compressed data, stored

data, or both.